УДК 004.772

В. М. Дорофеев[1] *

Автоматизация интеграции файлообменного решения в корпоративной вычислительной сети

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: Vlad.Dorofeev.b19-515@yandex.ru

Аннотация. Работа описывает процесс автоматизации интеграции файлообменного решения в корпоративную вычислительную сеть. Представлены основные задачи, возникающие при интеграции, а также рассматриваются возможные решения на основе использования современных технологий и инструментов автоматизации. В процессе работы исследуется предметная область, включая недостатки и уязвимости в работе базовых протоколов стека TCP/IP, а также недостатки и уязвимости файлообменных решений. Предложен новый способ интеграции файлообменного решения путем внедрения программного модуля автоматизированной конфигурации решения. В работе представлена программная реализация предлагаемого решения для автоматизированной интеграции файлообменного взаимодействия. Проведен анализ преимуществ и недостатков с точки зрения безопасности и отказоустойчивости. Областью применения данной работы являются корпоративные вычислительные сети, функционирующие на основе стека протоколов TCP/IP.

Ключевые слова: автоматизация, автоматизация файлообмена, SFTP-сервер, TCP/IP, корпоративная вычислительная сеть, Ansible, Vagrant

V. M. Dorofeev[1] *

Automation of a File-Sharing Solution Integration in a Corporate Computer Network

[1] National Research Nuclear University "MEPhI", Moscow, Russian Federation
* e-mail: Vlad.Dorofeev.b19-515@yandex.ru

Abstract. The paper describes the process of automating the integration of a file-sharing solution into a corporate computer network. The main tasks arising during integration are presented, as well as possible solutions based on the use of modern technologies and automation tools are considered. In the process of work, the subject area is investigated, including shortcomings and vulnerabilities in the operation of the basic protocols of the TCP/IP stack, as well as shortcomings and vulnerabilities of file-sharing solutions. A new way of integrating a file-sharing solution is proposed by introducing a software module for automated configuration of the solution. The paper presents a software implementation of the proposed solution for automated integration of file-sharing interaction. An analysis of the advantages and disadvantages from the point of view of security and fault tolerance is presented. The scope of this work are corporate computer networks operating on the basis of the TCP/IP protocol stack.

Keywords: automation, file sharing automation, SFTP server, TCP/IP, corporate computing network, Ansible, Vagrant

Введение

В настоящее время корпоративные вычислительные сети, реализованные на основе стека протоколов TCP/IP, являются неотъемлемой частью успешного функционирования современных компаний и государственных учреждений. Это объясняется их преимуществами, основанными на совместном использовании информации, обмене файлами между различными категориями пользователей: как между сотрудниками в пределах компании, так и между сотрудниками и контрагентами.

Увеличение объема информационных потоков сделало процесс передачи информации важной частью бизнес-процессов большинства организаций. Традиционные решения, такие как электронная почта и FTP, перестали удовлетворять широкому спектру требований, которые предъявляются к подсистеме безопасности компании. А использование сторонних неконтролируемых сервисов (общедоступные файлообменники) может привести к утечке конфиденциальной информации компании. Такие решения не способны обеспечить комплексную защиту передачи файлов, гарантировать конфиденциальность информации и контролировать процесс обмена. Также они слишком усложняют задачу, при этом в разы увеличивая расходы на ее решение.

Все это привело к тому, что компаниям теперь требуются продукты и решения, которые могут обеспечить полный контроль всего процесса файлообмена и управление им [1]. Всем вышеперечисленным условиям соответствует управляемая передача файлов, которую можно реализовать на базе привычного SFTP-сервера с его детализированной настройкой [2, 3] с помощью такого сильного инструмента как Ansible [4, 5]. Данное решение покрывает целый спектр задач, а именно: автоматизация передачи данных, безопасный и авторизованный обмен данными, обеспечение конфиденциальности передаваемой информации, обеспечение целостности файлов, управление пользователями и группами пользователей, интеграция с существующими информационными системами.

От выбранного файлообменного решения зависит эффективность, надежность и безопасность передачи информации. Неправильный выбор и настройка файлообменника могут привести к утечке конфиденциальных данных, к риску возникновения кибер-атаки. Соответственно возрастает потребность в разработке автоматизированного файлообменного решения для передачи и обмена данными [6, 7].

В рамках детального выявления проблематики необходимо провести исследование предметной области.

Исследование предметной области

Общий доступ к файлам и обмен файлами являются неотъемлемой частью функционирования любого предприятия и обеспечивают эффективность синхронизации данных и совместной работы между сотрудниками и подразделениями. Однако возрастает количество угроз безопасности, связанных с любым типом обмена файлами. По данным Национального координационного центра по ком-

пьютерным инцидентам (НКЦКИ) с февраля 2022 года уровень угрозы кибератак на информационные ресурсы – критический. Это показывает, что большинство современных информационных систем (ИС) не соответствуют широкому спектру выдвигающихся к ним требований.

Основными рисками при передаче и общем доступе к данным являются раскрытие конфиденциальных данных, уязвимость к кибератакам, загрузка вредоносного программного обеспечения (ПО).

На данный момент большинство компаний выбирают облачные сервисы для организации общего доступа сотрудников к информации. Облачный общий доступ к файлам позволяет легко отправлять файлы и совместно с командой работать над одним документом. Облачные хранилища обладают довольно высокой степенью защищенности. Однако по данным экспертно-аналитического центра InfoWatch за 2021 год из облачных хранилищ были скомпрометированы персональные данные 3,58 млрд человек. Данное исследование подтверждает необходимость создания защищенного файлообмена внутри корпоративной вычислительной сети предприятия. Компании лучше всего иметь свои собственные физические серверы для обеспечения процесса файлообмена. Таким образом, компании смогут сами контролировать серверы и путем корректной настройки оборудования и автоматизации процесса передачи смогут обеспечить полный контроль всего процесса файлообменного взаимодействия, исключить возможные человеческие ошибки при отправке данных, что позволит повысить конфиденциальность, целостность и доступность информации.

Также согласно исследованиям [8, 9] при разработке информационной системы современных предприятий важным аспектом является автоматизация процессов файлообменного взаимодействия. С помощью автоматизации данного процесса можно детально сконфигурировать файлообмен внутри корпоративной вычислительной сети и обеспечить высокий уровень информационной безопасности предприятия.

Постановка задачи

Целью настоящей работы является обеспечение безопасности передачи данных в корпоративной вычислительной сети путем внедрения программного модуля автоматизации файлообменного взаимодействия. В ходе решения данной проблемы выделены следующие задачи:

– исследование предметной области;
– проектирование алгоритма предлагаемого решения;
– программная реализация решения;
– проведение автоматизированного тестирования разработанного решения.

Предлагаемое решение

Предлагаемое решение основано на реализации безопасного файлообмена внутри корпоративной вычислительной сети и дальнейшей автоматизации конфигурирования. Для обеспечения безопасной передачи информации внутри компании были выбраны и решены следующие задачи:

– конфигурирование VPN-соединения;
– обновление системы;
– смена портов SSH;
– проверка работоспособности после смены портов;
– настройка SELinux;
– создание группы пользователей;
– создание пользователей;
– настройка доступа пользователей к каталогам;
– обновление паролей пользователей;
– создание директории для логирования.

В ходе работы был спроектирован оригинальный алгоритм (рис. 1) работы предлагаемого решения. Данный алгоритм включает в себя нетривиальные задачи, на которые уходит большое количество времени в ходе ручного конфигурирования инфраструктуры.

При разработке алгоритма учитывались требования к безопасности корпоративной вычислительной сети. Безопасность достигалась за счёт применения VPN-соединения, это позволило шифровать весь входящий и исходящий трафик на SFTP-сервере. Использование VPN-соединения может защитить от атак типа «человек посередине». Атакующий позиционирует себя в середине соединения и пытается перехватить трафик. Данный тип атаки распространен в общедоступных сетях Wi-Fi. VPN в свою очередь шифрует соединение, следовательно, IP-адрес и трафик будут зашифрованы, и злоумышленник не сможет их перехватить.

Также в алгоритм заложена смена порта SSH, что является немаловажной частью для обеспечения безопасности SFTP-сервера. Смена портов по умолчанию позволяет защититься от DDoS-атак и брутфорс. Злоумышленник будет стучаться на определённый порт, но так как произошла смена, то все его попытки будут напрасны и сервер будет функционировать в прежнем режиме.

При разработке программного модуля использовалось средство автоматизации Ansible. Данное решение покрывает целый спектр задач, а именно: автоматизация передачи данных, безопасный и авторизованный обмен данными, обеспечение конфиденциальности передаваемой информации, обеспечение целостности файлов, управление пользователями и группами пользователей, интеграция с существующими информационными системами.

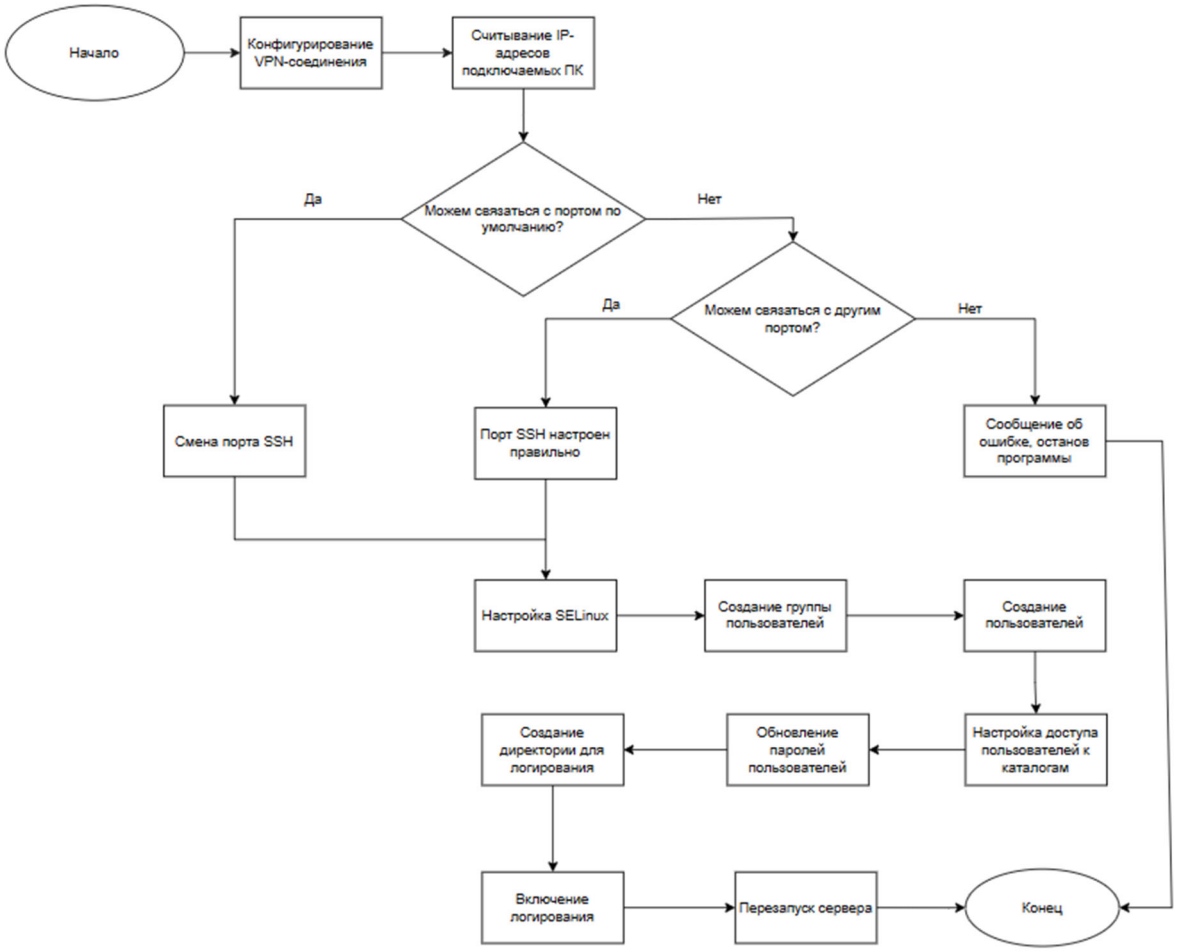

Рис. 1. Алгоритм работы программного модуля

Экспериментальное исследование

В рамках экспериментального исследования была поднята экспериментальная сеть, состоящая из физического SFTP сервера, на котором был установлен VPN и 3 виртуальные машины (рис. 2), которые находятся под управлением Vagrant (рис. 3).

Один из изображенных на рис. 2 узлов является SFTP-сервером, остальные три виртуальные машины выступают в роли пользователей корпоративной вычислительной сети. Каждый пользователь проходит автоматизированную конфигурацию и подключение к SFTP-серверу.

В рамках экспериментального исследования было проведено модульное тестирование предлагаемого решения. Модульное тестирование проводилось при помощи встроенных механизмов и дополнительного программного средства (ПС) *Molecule*. Модульное тестирование – это процесс тестирования отдельных компонентов программного обеспечения (модулей) с целью выявления дефектов и проверки работоспособности каждого модуля в изоляции от других компонентов. Каждый модуль тестируется отдельно, используя различные методы тести-

рования. Цель модульного тестирования – обеспечить быстрое обнаружение и исправление ошибок в каждом модуле, что повышает надежность и качество всей системы в целом.

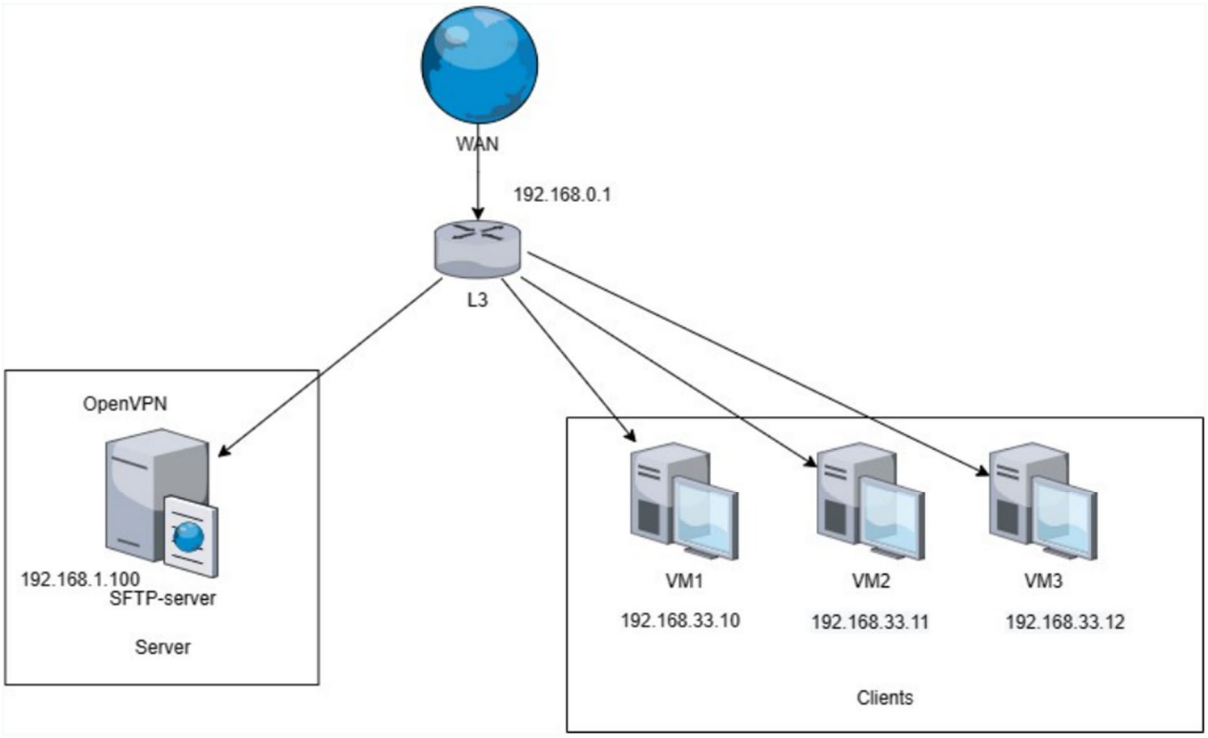

Рис. 2. Схема экспериментальной сети

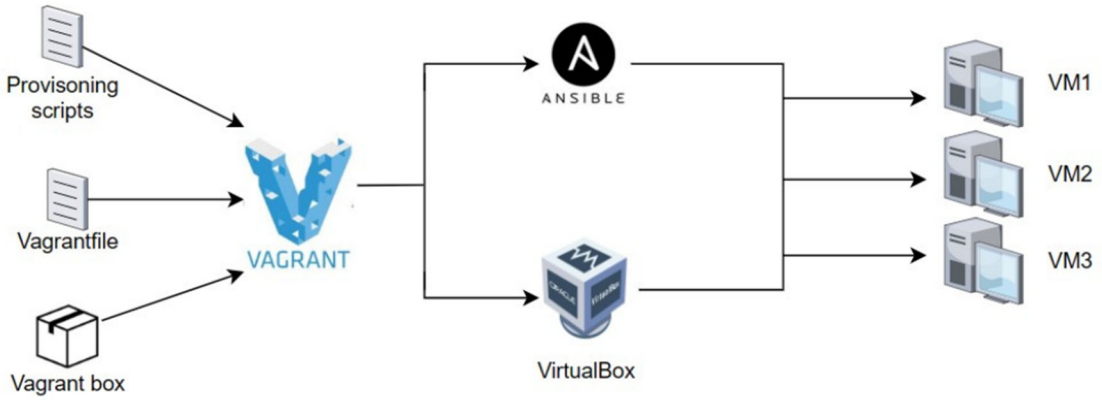

Рис. 3. Схема работы Vagrant

По результатам тестирования предлагаемое решение успешно продемонстрировало реализацию безопасного файлообмена с применением методов автоматизации, а также показало отсутствие уязвимостей исходного кода.

Заключение

В рамках данной работы было предложено решение, основанное на реализации безопасного файлообмена внутри корпоративной вычислительной сети и

дальнейшей автоматизации конфигурирования, которое было реализовано программно и хорошо показало себя на этапе тестирования.

Практическая значимость работы состоит в повышении безопасности информационной инфраструктуры предприятия и устранении ошибок ее ручного конфигурирования.

Новизна данной работы состоит в предложении нового алгоритма развертывания инфраструктуры и ее дальнейшего сопровождения, повышающего надежность, отказоустойчивость и информационную безопасность развертываемой инфраструктуры предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Basinya E. A. Automatic traffic control system for SOHO computer networks / E. A. Basinya, A. A. Rudkovskiy // Studies in Systems, Decision and Control. - 2019. - Vol. 119 : Recent Research in Control Engineering and Decision Making. ICIT 2019. - P. 743-754. - DOI: 10.1007/978-3-030-12072-6_60.

2. Basinya E. A. An automated system of network and system administration of Windows and Linux family operating systems = Автоматизированная система сетевого и системного администрирования операционных систем семейства Windows и Linux / E. A. Basinya // Научный вестник Новосибирского государственного технического университета. - 2018. – № 4 (73). – С. 47–58. - 300 copy - DOI: 10.17212/1814-1196-2018-4-47-58.

3. Basinya E. A. An automated system of network and system administration of Windows and Linux family operating systems = Автоматизированная система сетевого и системного администрирования операционных систем семейства Windows и Linux / E. A. Basinya // Научный вестник Новосибирского государственного технического университета. - 2018. – № 4 (73). – С. 47–58. - 300 copy - DOI: 10.17212/1814-1196-2018-4-47-58.

4. А. Зензинов Automated deployment of virtualization-based research models of distributed computer systems // Proceedings of the Spring/Summer Young Researchers' Colloquium on Software Engineering, 2013 г

5. Пранав Т.П., Чаран С., Даршан М.Р., Гириш Л., «Методы DevOps для автоматизации управления серверами с использованием Ansible International Journal of Advanced Scientific Innovation», том 01, выпуск 02, май 2021 г.

6. Павел Масек, Мартин Стусек, Ян Крейчи, Кристоф Земан, Иржи Покорны и Марек Кудлачек, «Раскрытие полного потенциала Ansible Framework: администрирование университетских лабораторий», Software Engineering Companion (ICSE-C), 2021 IEEE/ACM, 39-я международная конференция on, стр. 497–498, IEEE, 2021.

7. Супрунов С. Автоматизируем FTP с помощью Python //Системный администратор. 2004. № 12 (25). С. 36-41.

8. Мохд Фарис Мохд Фузи, К. Абдулла, Иман Хазвам Абд Халим, «Автоматизация сети с использованием Ansible для сети EIGRP», Журнал вычислительных исследований и инноваций, том 05, выпуск 03, 20 сентября 2021 г.

9. Косенков В.В., Богданов А.В. Автоматизация настройки сервера с помощью Ansible //Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации. Сборник статей LIX Международной научно-практической конференции. Пенза, 2022. С. 32-36.